CIBERSEGURIDAD

‘Bootcamp IX’

Informe Práctica Módulo Recopilación de Información.

Maximiliano Dariel Altamirano.

Academia KeepCoding.

INDICE

[INFORME 3](#_Toc192104232)

[Descripción de la práctica 3](#_Toc192104233)

[Descripción del dominio 3](#_Toc192104234)

[FOOTPRINTING 4](#_Toc192104235)

[Análisis activo 4](#_Toc192104236)

[Análisis pasivo 7](#_Toc192104237)

[FINGERPRINTING 9](#_Toc192104238)

[ANALISIS DE VULNERABILIDADES 17](#_Toc192104239)

[OSINT 23](#_Toc192104240)

[RESUMEN 29](#_Toc192104241)

[Objetivo 29](#_Toc192104242)

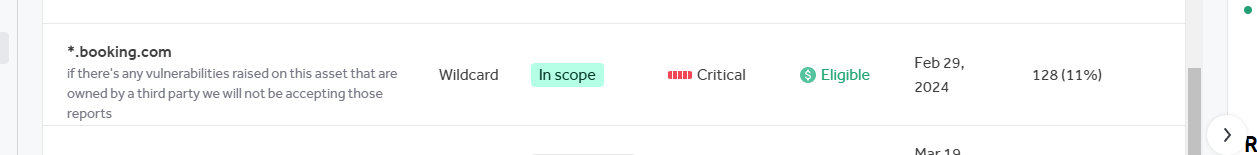
[Herramientas 29](#_Toc192104243)

# INFORME

### Descripción de la práctica

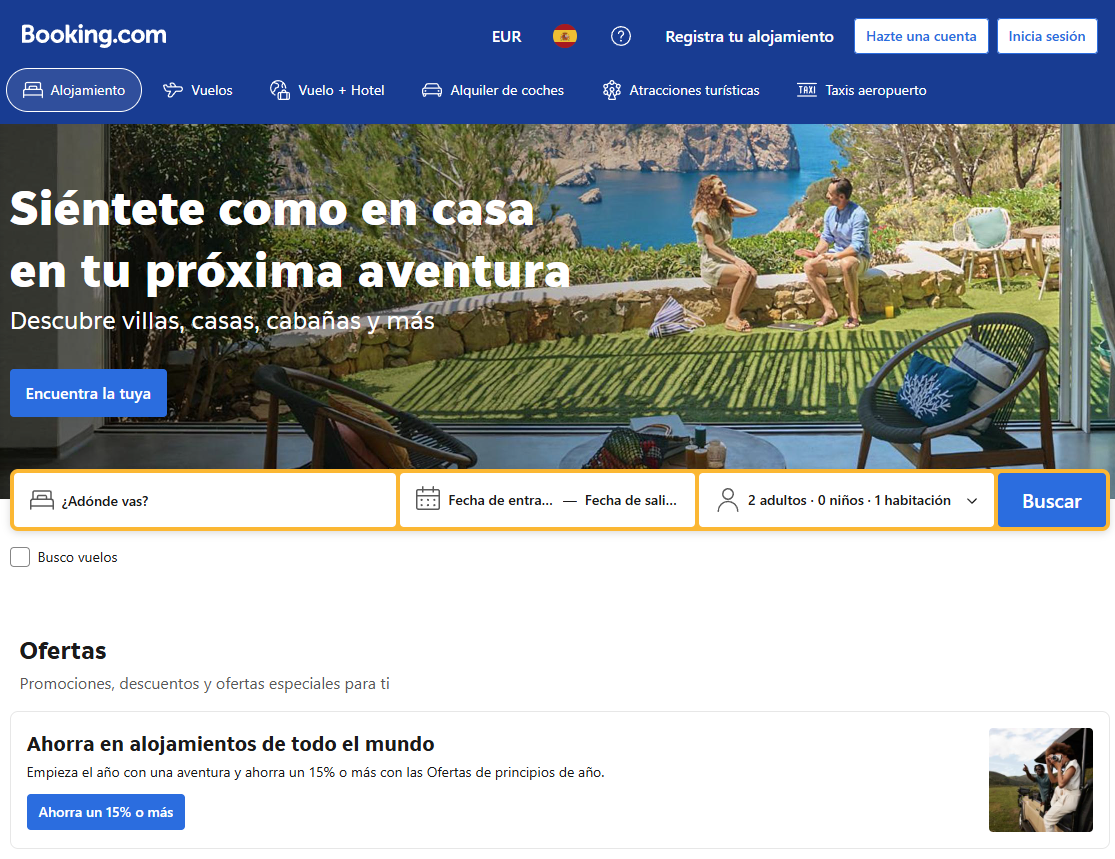
Para el desarrollo de la práctica realizaremos la recopilación de datos sobre el dominio **www.booking.com,** elegido por su scope amplio respetando las normas y condiciones de la plataforma www.hackerone.com.

Intentaremos identificar Bugs y Vulnerabilidades del dominio mencionado.



### Descripción del dominio

**Booking.com** es una plataforma de reservas de alojamientos y tarifa de viajes, fue fundada en Países Bajos en 1996 y forma parte de Booking Holding Inc.



Abordaremos las diferentes etapas de la recopilación de datos con la siguiente estructura:

* Footprinting
* Fingerprinting
* Análisis de Vulnerabilidades
* OSINT

Como ejes principales de nuestro informe.

# FOOTPRINTING

En este apartado intentaremos identificar los subdominios con reconocimiento vertical de nuestra Web objetivo, utilizando técnicas activas y pasivas.

### Análisis activo

Utilizaremos **Shuffledns** para identificar los posibles subdominios de nuestra Web objetivo con fuerza bruta, lanzamos el siguiente comando:

shuffledns -mode bruteforce -d booking.com -w $HOME/recopilacion/lists/domains.txt -r $HOME/recopilacion/lists/resolvers.txt -silent > shuffledns.txt

En este primer informe identificamos 94 subdominios, de los cuales marcaremos como relevantes:

**secure.booking.com**: Este dominio podría estar relacionado con la seguridad y autenticación.

**developer.booking.com**: Podría proporcionar información sobre APIs y recursos para desarrolladores.

**api.booking.com**: Este dominio probablemente esté relacionado con las APIs de Booking.com.

**admin.booking.com**: Podría estar relacionado con la administración interna del sitio.

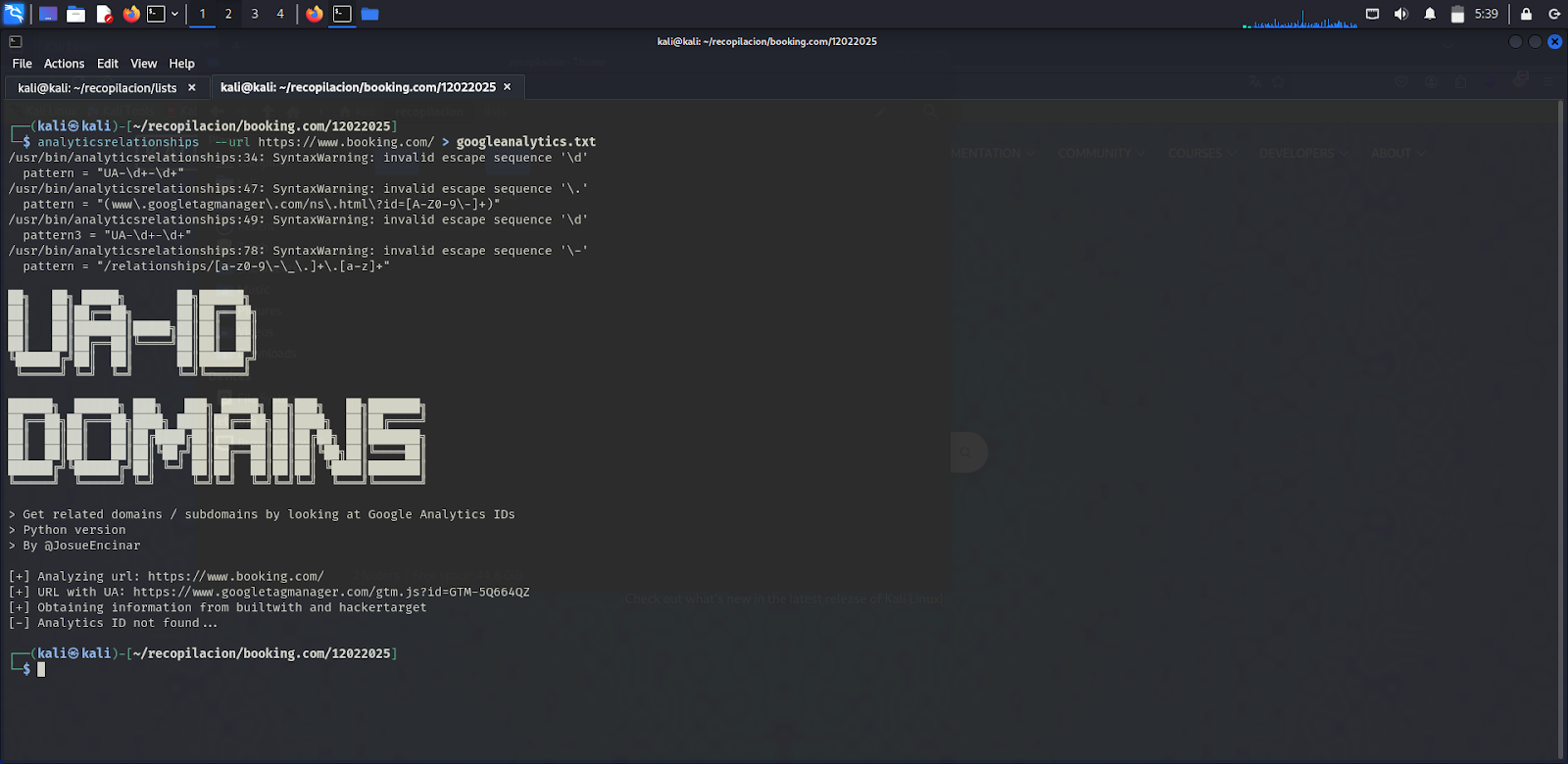
**bugs.booking.com**: Podría ser un dominio utilizado para reportar y rastrear errores, útil para conocer el procedimiento ante tipo de problemática.

**jira.booking.com**: Podría estar relacionado con el sistema de seguimiento de problemas y proyectos de Booking.com.

**vpn.booking.com**: Este dominio podría estar relacionado con la red privada virtual (VPN) de Booking.com.

Analizamos con **Analyticsrelationships** si nuestra Web objetivo tiene definido un ID de Google Analytics:

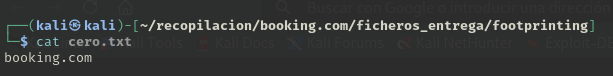
analyticsrelationships --url <https://www.booking.com/>



En esta oportunidad nuestra Web objetivo no cuenta con ID para progresar en el análisis.

Exploramos los certificados SSL/TLS con la herramienta **Cero** intentando identificar los dominios y subdominios que puedan pertenecer a la organización objetivo relacionados a estos certificados. Lanzamos el siguiente comand:

cero -d booking.com | grep 'booking.com' > cero.txt



Nuestro análisis solo a identificado el dominio principal, sin datos que destacar.

Utilizamos la técnica de Web Scraping para extraer información de nuestra Web objetivo con la herramienta **Katana** y **Unfurl** para obtener los subdominios de la url. lanzaremos el siguiente comando:

echo booking.com | katana -jc -o katanaoutput.txt -kf robotstxt, sitemapxml | unfurl --unique domains > katana.txt

Hemos identificado 19 subdominios, ninguno trascendente para destacar ya que algunos datos los hemos mencionado en el primer análisis.

### Análisis pasivo

Revisaremos los certificados asociados a la Web objetivo con la intención de identificar los subdominios vinculados a estos logs, para ello utilizaremos la herramienta **CTFR** lanzando el siguiente comando:

ctfr -d booking.com | unfurl --unique domains > ctfr.txt

Encontramos 947 subdominios, de los cuales podemos destacar la siguiente información:

**tls12-secure-distribution-xml.booking.com // tls12-secure-supply-xml.booking.com**: Subdominios interesantes para evaluar configuraciones de TLS, certificados SSL y posibles vulnerabilidades.

**ams4.dev.booking.com, \*.dev.booking.com, dev.booking.com:** Entonces de producción, suelen configurarse con menos seguridad que un entorno de producción.

**gdpr.support.booking.com:** Posiblemente relacionado con cumplimiento legal y protección de datos (GDPR).

Solo como dato adicional, sumaremos un fichero con los certificados asociados a la organización “Booking” modificando parámetros de la herramienta y lanzando el siguiente comando:

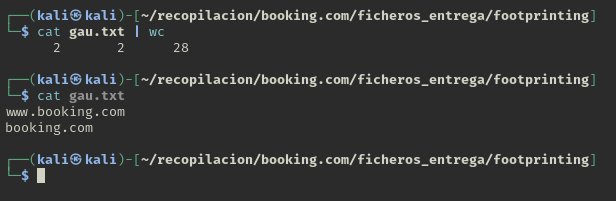
ctfr-org -d Booking > ctfr-org.txt



Descubrimos 401 dominios y subdominios relacionados a la organización.

Haremos un reconocimiento sobre los archivos Web y Cache de nuestra Web Objetivo utilizando la herramienta **GAU**, lanzamos el siguiente comando:

gau --threads 5 booking.com --o gauoutput.txt --timeout 4 | unfurl --unique domains > gau.txt



Para este apartado solo hemos identificado 2 dominios luego de 4hs de análisis de la herramienta, sin datos que destacar.

Unificamos todos los subdominios en un solo fichero denominado presubdominios.txt:

cat cero.txt ctfr.txt gau.txt katana.txt shuffledns.txt > presubdominios.txt

Con la información obtenida haremos permutaciones a los subdominios recolectados. También identificaremos de la nueva lista que subdominios se encuentran activos, por lo que utilizaremos las herramientas **ALTERX** y **DNSX** para contar con una base funcional. Lanzaremos el siguiente comando:

cat subdominios.txt | alterx | dnsx > alterx.txt

Para finalizar nuestro Footprinting vamos a concatenar toda la información recolectada con diferentes técnicas en el fichero denominado subdominios.txt

cat presubdominios.txt alterx.txt > subdominios.txt

En resumen, utilizaremos el fichero “***subdominios.txt***” como referencia, con sus 1261 subdominios encontrados, como parámetros en los siguientes análisis.

# FINGERPRINTING

Para este apartado intentaremos descubrir información específica de nuestra Web objetivo, como tecnologías, puertos que utilizan sus servidores, sistema operativo, posibles waf entre otros. Para ello implementaremos varias herramientas automatizadas y también haremos recolección manual de información.

Gestionaremos con la herramienta **HTTPX** para identificar los dominios que se encuentran “online” en nuestra base, lanzaremos el siguiente comando:

cat subdominios.txt | httpx -silent | unfurl --unique domains > subdominiosfinal.txt

Así logramos identificar 291 subdominios online, sumaremos al listado de hallazgos el siguiente subdominio:

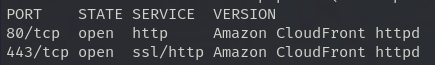
**account.booking.com**: Este subdominio podría ser de administración y gestión de cuentas.

Transformaremos nuestra base de subdominios DNS a fichero de IPs para realizar el scanner con la herramienta Masscan:

for subdominio in $(cat subdominiosfinal.txt); do dig +short $subdominio | grep -Eo '([0-9]{1,3}.){3}[0-9]{1,3}'; done > subdominiosfinal\_ips.txt

Antes lanzaremos **Nmap** solo sobre el dominio principal para identificar los puertos abiertos y optimizar el scanner de Masscan con el siguiente comando:

sudo nmap -Pn -sS -sV -p0- booking.com > nmap.txt

Ya identificando los puertos abiertos intentaremos configurar los parámetros de manera más eficiente:  
  


Ocupamos **Masscan** y sumaremos, a los parámetros ya encontrados, los puertos más importantes para intentar identificar el acceso a puertos críticos:

sudo masscan -p22,25,53,80,443,3389,3306,1433,3389,8443 -iL subdominiosfinal\_ips.txt > masscan.txt

En los resultados obtenidos no encontramos información trascendente más que los esperados, ya que el análisis muestra de manera redundantes los puertos 443 y 80.

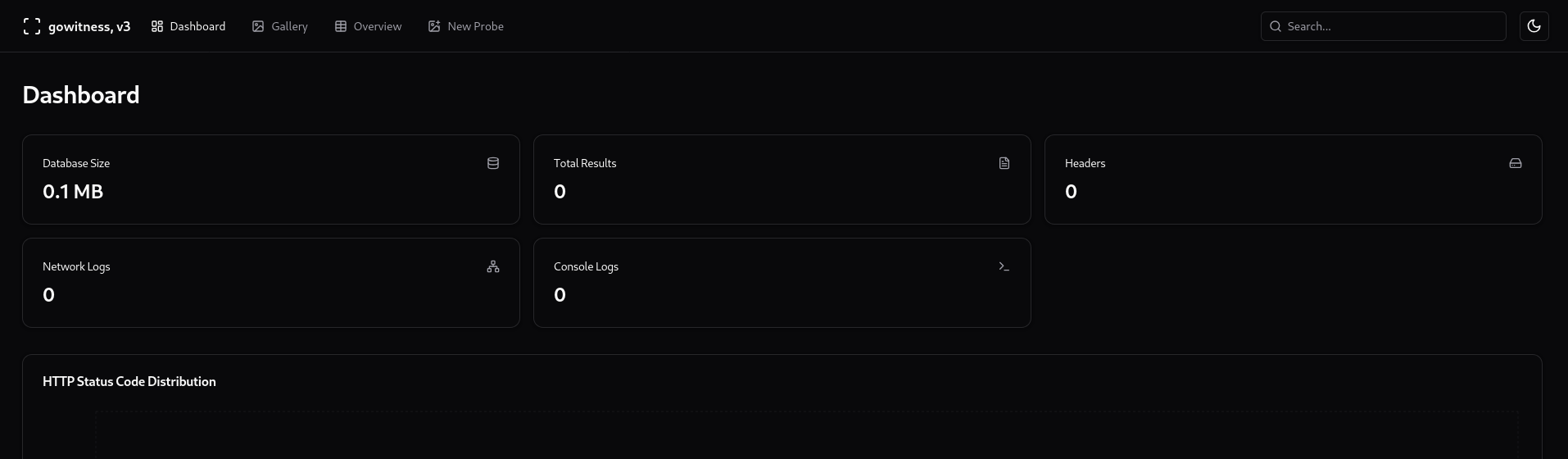
Utilizaremos la herramienta GoWitness para realizar capturas de pantalla de los subdominios encontrados con el siguiente comando:

gowitness scan file -f subdominiosfinal.txt

Aprovecharemos la interfaz de la herramienta para revisar los resultados desde, utilizamos el comando

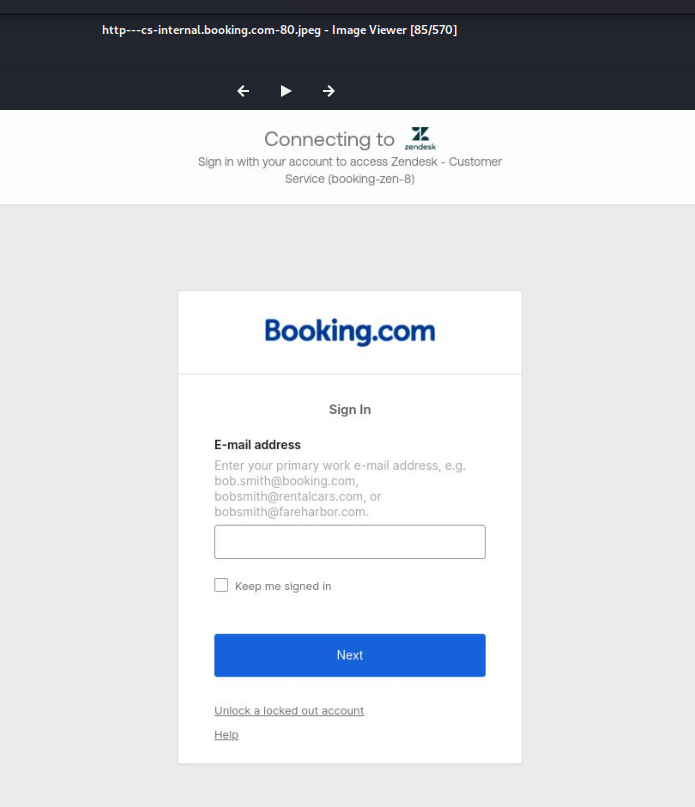
gowitness report server

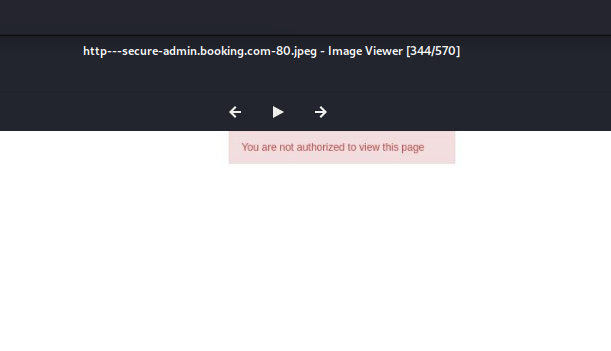
Y accedemos al servidor <http://localhost:7171/>

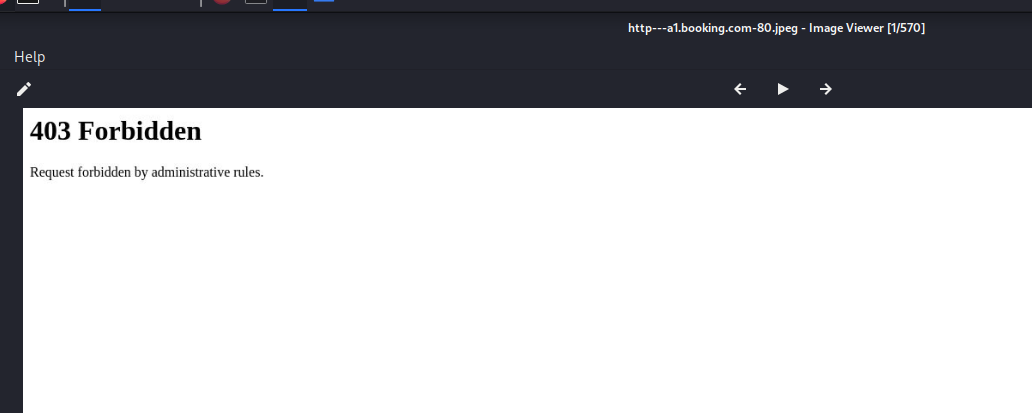


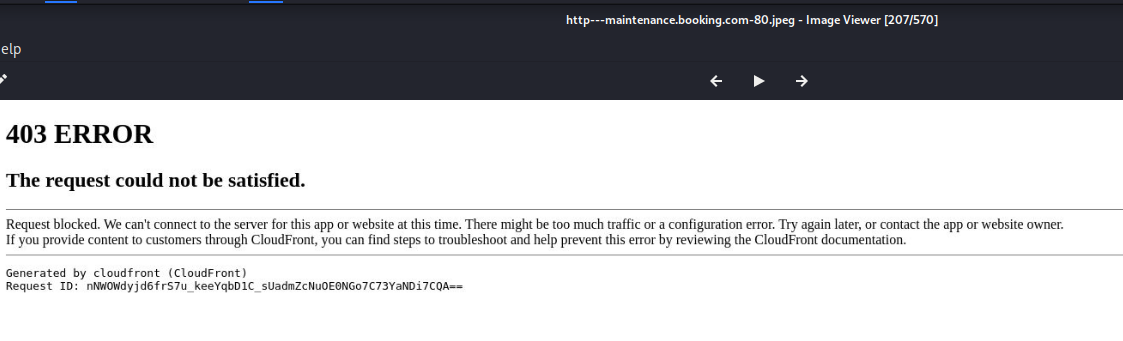
Al no disponer de información la interfaz de la herramienta (sin actualización en la herramienta), haremos una exploración manual sobre las capturas de pantalla recolectadas en busca de indicios de vulnerabilidades.





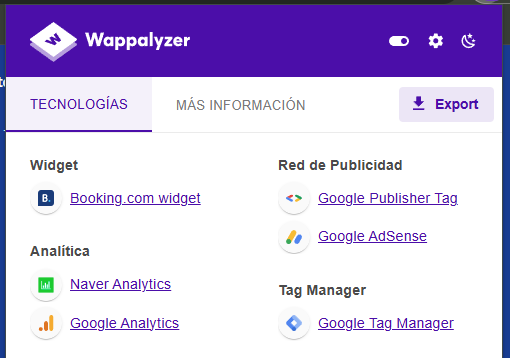


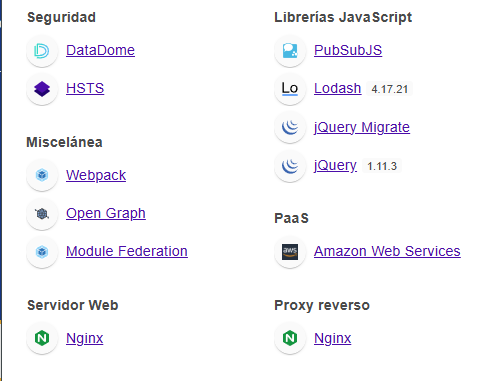


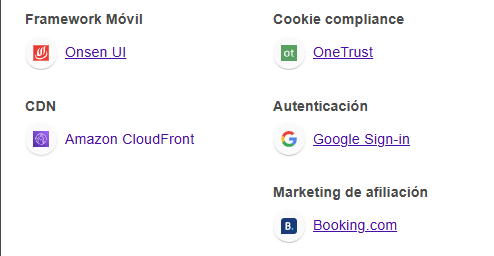


El error puede que visualizamos puede deberse a un tráfico excesivo o a una configuración incorrecta, ya que es recurrente el error en nuestras evidencias.

Sumaremos información con **Wapallyzer** de las tecnologías que utiliza nuestra Web objetivo.







Destacaremos las siguientes tecnologías utilizadas:

Fortaleza:

**DataDome**: Generalmente usado para protección contra bots maliciosos, mitigación de ataques de scraping y protección frente a tráfico automatizado.

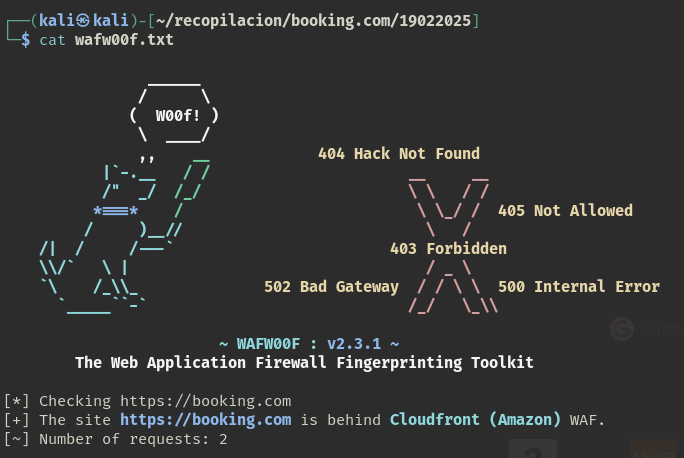
**HSTS (HTTP Strict Transport Security)**: Añade una capa de seguridad al forzar el uso de conexiones HTTPS y prevenir ataques como "SSL stripping".

Oportunidad de mejora:

**Webpack**: Un empaquetador de módulos JavaScript, podría tener dependencias que necesitan auditorías regulares para identificar vulnerabilidades.

Identificaremos si nuestro objetivo está detrás de un Waf utilizando la herramienta **Waf00f** lanzando el siguiente comando.

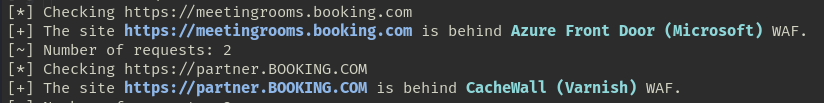
wafw00f booking.com > wafw00f.txt



Podemos visualizar que **Cloudfront (Amazon)** es el Waf elegido por Booking para su dominio principal.   
  
Haremos en scanner a nuestro fichero de subdominios con **Waf00f** para identificar más información sobre los Waf que utiliza la organización.







Identificamos otros servicios Waf como Azure Front Door, Envoy, Cloudflare y CacheWall.

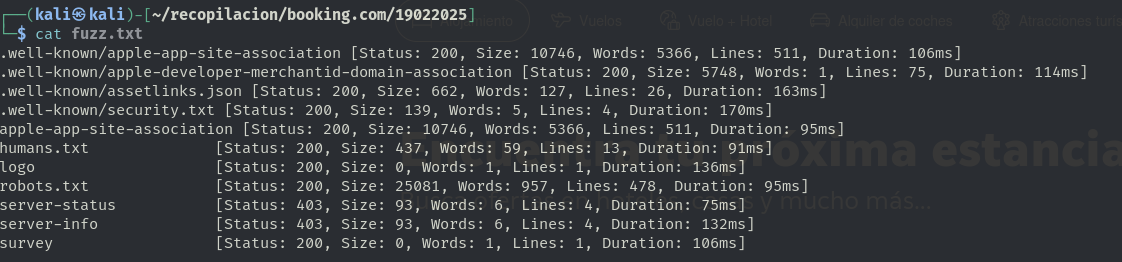
Intentaremos realizar un descubrimiento de contenidos utilizando la herramienta **ffuf**, lanzaremos el siguiente comando configurando los parámetros necesarios. En primera instancia utilizaremos la lista de palabras common.txt descargada del siguiente repositorio:

get https://raw.githubusercontent.com/danielmiessler/SecLists/refs/heads/master/Discovery/Web-Content/common.txt

Ya con el listado completo, lanzamos el siguiente comando:

ffuf -w ~/recopilacion/lists/common.txt -t 10 -mc 200,401,403 -u https://booking.com/FUZZ

Varios de los directorios descubiertos pueden ser objetivo de fuerza bruta.

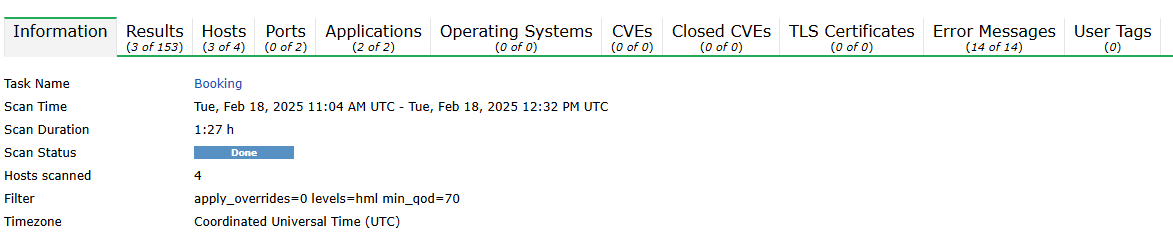


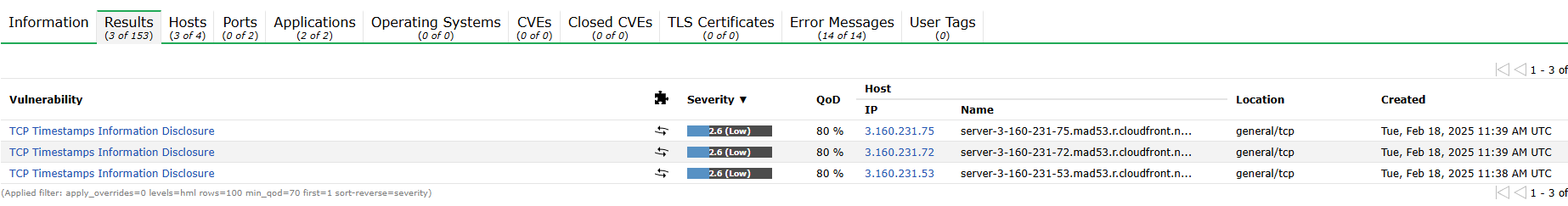
En resumen, nuestra Web objetivo implementa tecnologías y puertos configurados de forma correcta, gestionando con diferente Waf de confianza.

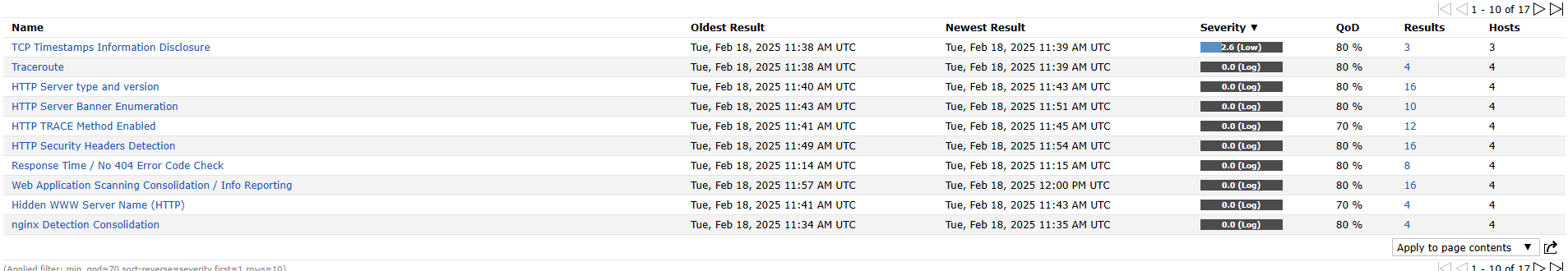
# ANALISIS DE VULNERABILIDADES

Para este apartado utilizaremos diferentes herramientas de análisis, comenzaremos con **Greenbone**, gestionaremos la información de manera local desde el navegador.









Revisando los resultados obtenidos, podemos concluir que nuestra Web objetivo tiene un grado de severidad **Bajo** a vulnerabilidades criticas conocidas, dificultando el acceso a terceros.

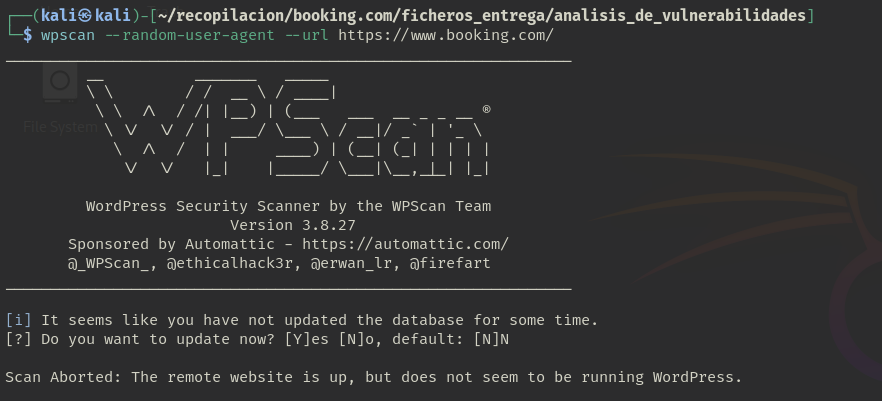
Realizamos un nuevo análisis con la herramienta **Nuclei**, lanzamos el siguiente comando:

nuclei -u booking.com > nuclei.txt

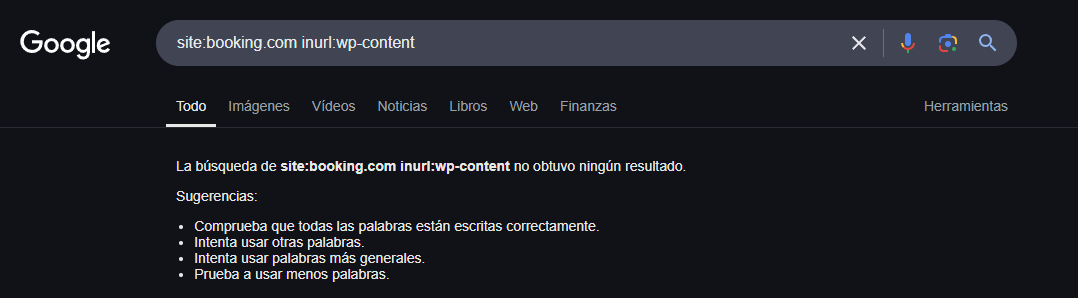
Luego del análisis y al revisar la información, podemos afirmar que las configuraciones y tecnologías implementadas son seguras.

Utilizaremos la herramienta WPScan para identificar si se utiliza WordPress. Lanzaremos el siguiente comando:

wpscan --random-user-agent --url https://www.booking.com/

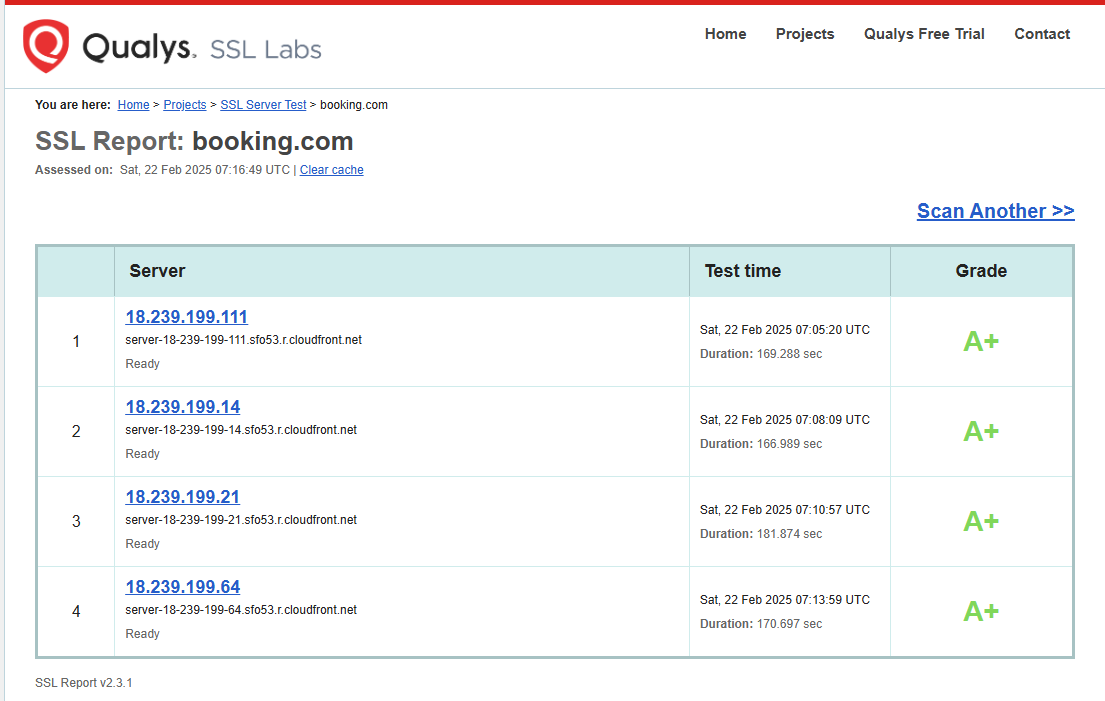


Confirmamos que no corre WordPress con una simple búsqueda en el navegador “site:booking.com inurl:wp-content”



Analizaremos con **Qualys** los certificados TLS/SSL de nuestra Web objetivo:

<https://www.ssllabs.com/ssltest/analyze.html?d=booking.com>

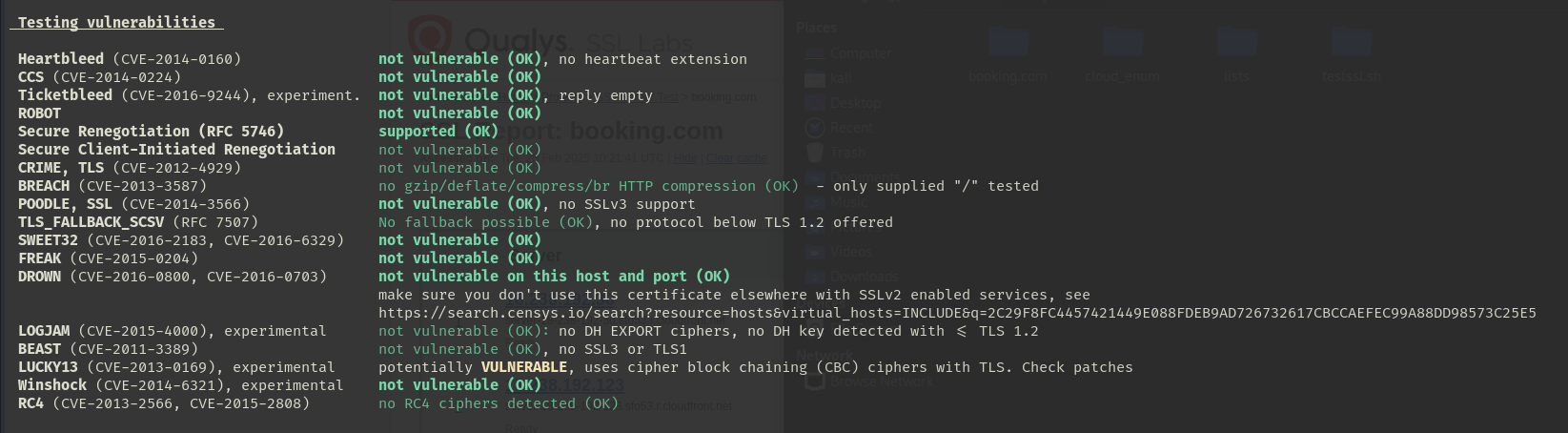


También haremos las comprobaciones por consola con la herramienta **testssl** lanzando el siguiente comando:

./testssl.sh booking.com > testssl.txt

Del informe generado podemos destacar una potencial vulnerabilidad:

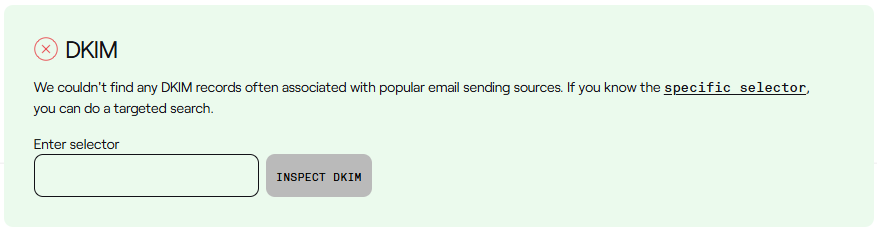
LUCKY13 (CVE-2013-0169): Potencialmente vulnerable, se utilizan cifrados CBC (Cipher Block Chaining) con TLS. Se recomienda revisar parches de seguridad.



Ejecutamos un análisis sobre los servicios de correo electrónico desde la siguiente web <https://dmarcian.com/>, logrando los siguientes resultados:



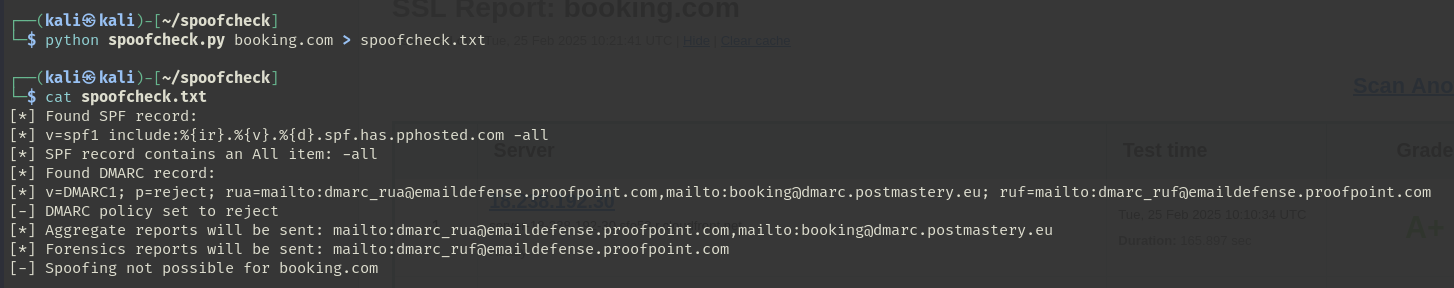
La misma no ha encontrado registros DKIM para la organización analizada.



Podemos comprobar que el dominio principal utiliza registros validos de DMARC y SPF.

Replicaremos las comprobaciones desde consola utilizando la herramienta **spoofcheck.py**,lanzando el siguiente comando:

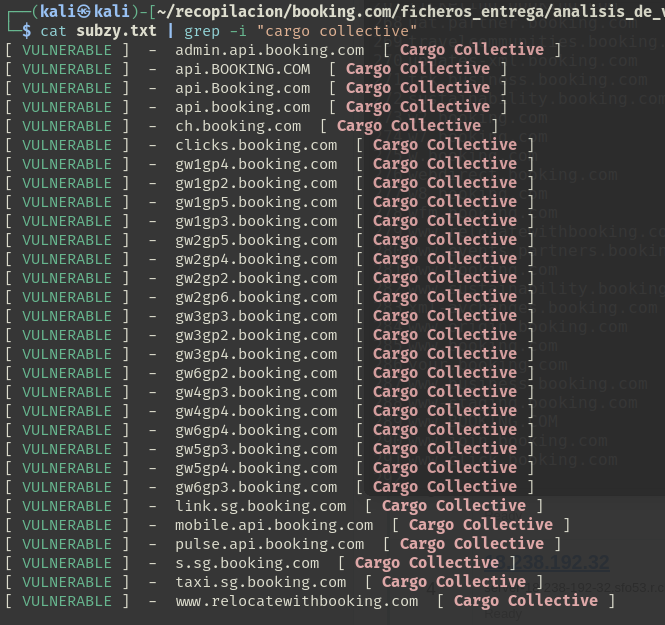
* python spoofcheck.py booking.com > spoofcheck.txt



Con estos datos, validamos que no es posible hacer Spoofing sobre nuestra Web objetivo.

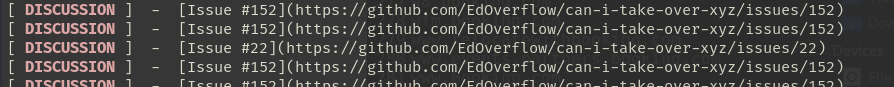
Para finalizar nuestro análisis de vulnerabilidades, vamos a explorar los posibles Subdomain Takeover con la herramienta **Subzy**. Lanzaremos el siguiente comando:

* subzy run --targets subdominiosfinal.txt > subzy.txt las siguientes vulnerabilidades:



De los resultados obtenidos podemos destacar dos posibles vulnerabilidades potenciales:

[ DISCUSSION ] - [Issue #152](https://github.com/EdOverflow/can-i-take-over-xyz/issues/152)

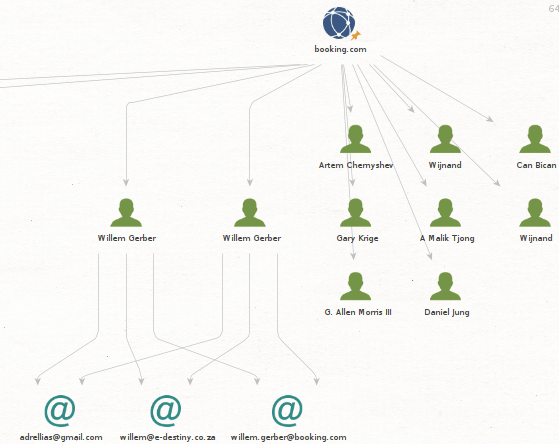
[ DISCUSSION ] - [Issue #22](https://github.com/EdOverflow/can-i-take-over-xyz/issues/22)  
  


Resumiendo, luego del análisis de realizado con diversas técnicas y herramientas podemos concluir que nuestra Web objetivo utiliza protocolos de seguridad altos y tecnologías seguras, siento un objetivo difícil de atacar también en este apartado.

# OSINT

Respecto a este punto haremos una recopilación de datos de fuentes públicas, utilizaremos navegadores y técnicas automatizadas para la práctica.

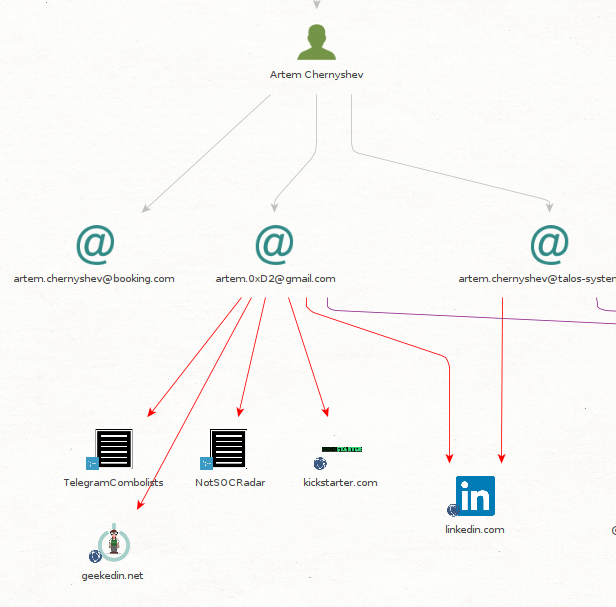
Lanzamos un análisis de la organización con la herramienta **Maltego**, en primera instancia haremos transformaciones buscando identificar personas relacionadas al dominio, posibles empleados. Utilizaremos el módulo “Email Addresses from Person” luego de identificar personas vinculada con la organización.

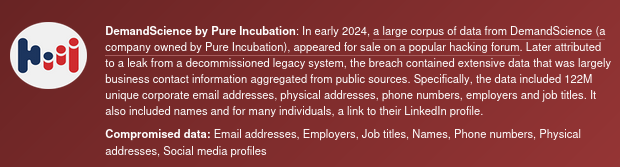
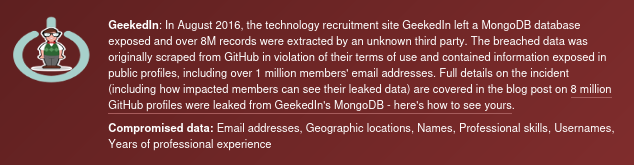
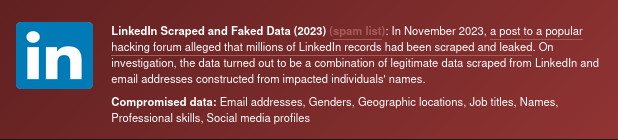


Aunque no disponemos del rol o función en la organización de cada figura descubierta, podemos identificar un perfil asociado a desarrollador, como lo es **Artem**.  
  
Analizaremos los correos electrónicos asociados a esta persona (posible empleado de la organización) en *https://haveibeenpwned.com/*:

* [artem.chernyshev@booking.com](mailto:artem.chernyshev@booking.com)
* [artem.0xD2@gmail.com](mailto:artem.0xD2@gmail.com)
* [artem.chernyshev@talos-systems.com](mailto:artem.chernyshev@talos-systems.com)

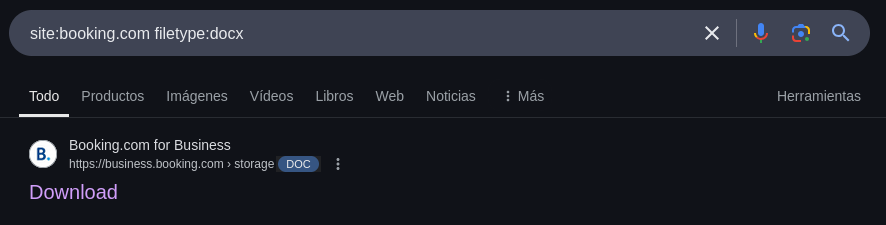
Podemos destacar las siguientes entidades asociadas vulneradas asociadas a dichos correos, comprometiendo información sensible.

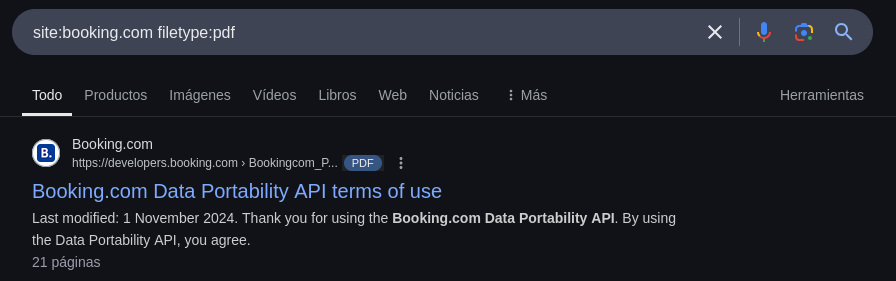




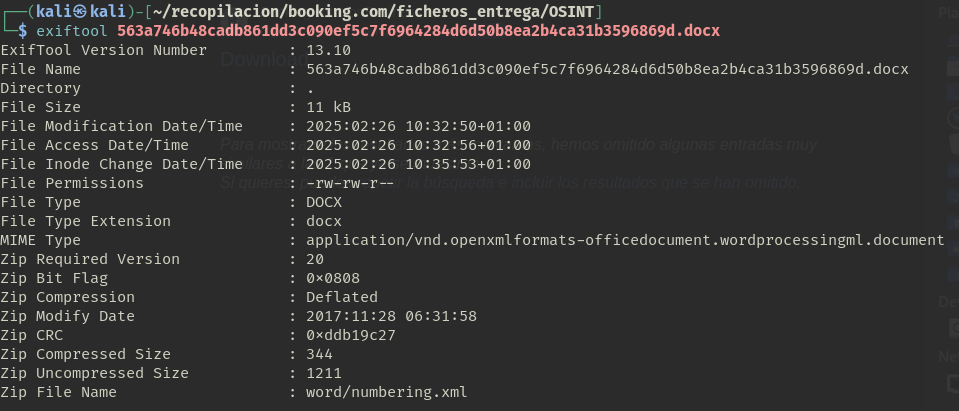
Este tipo de información es importante para conocer el comportamiento interno y los procedimientos conocidos por los empleados de la organización ante escenarios de phishing.

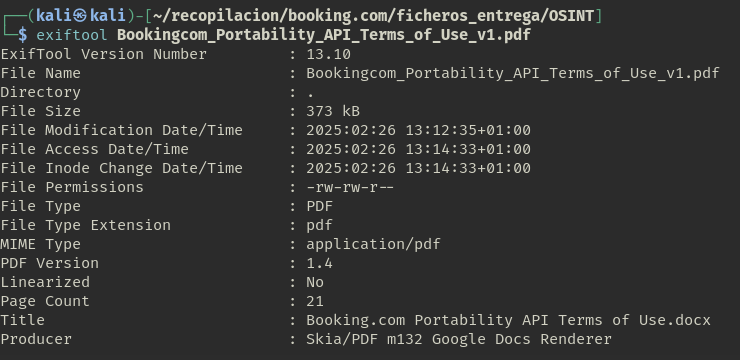
Avanzaremos con una búsqueda de fichero compartidos expuestos en internet de diferentes formatos conocidos, como docx, xlsx, ppt, pdf:





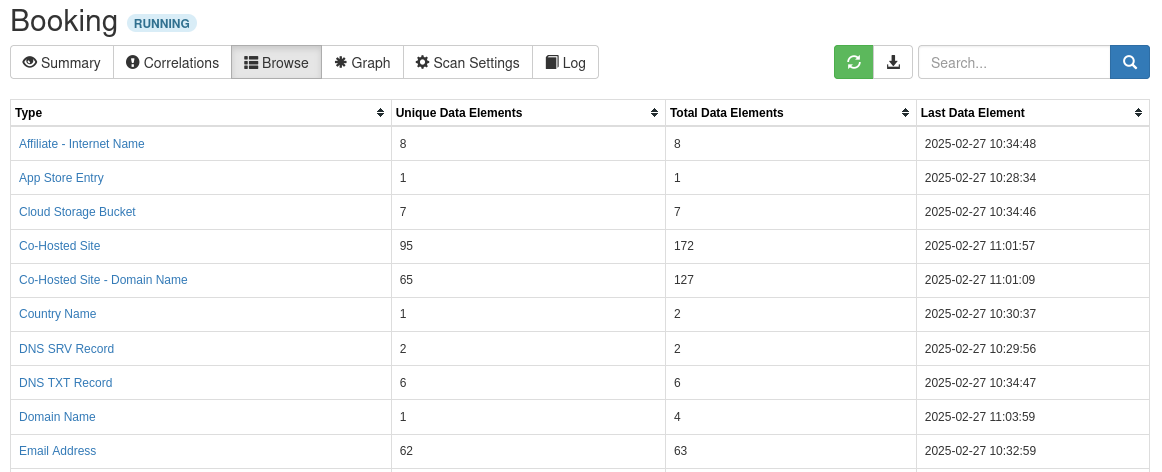
Analizaremos los archivos descargados con **exiftool**





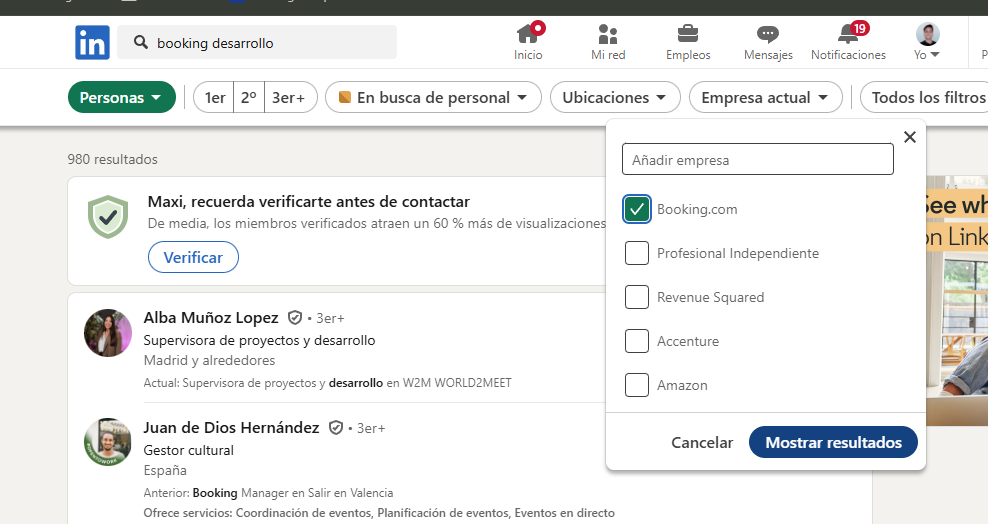
Los datos resultantes no aportan información trascendente, ya que no hay información de versiones o usuarios.

Utilizaremos la plataforma **Spiderfoot** para un nuevo análisis del dominio:

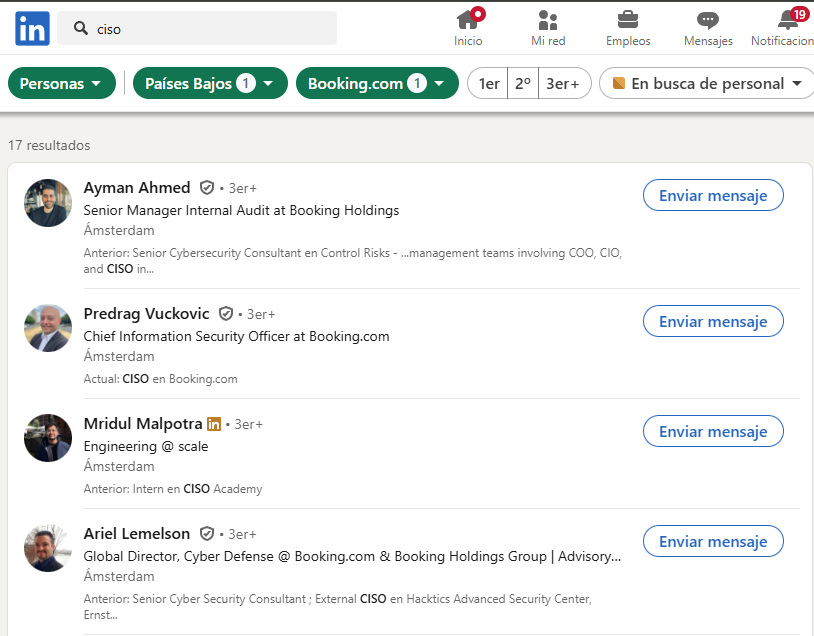


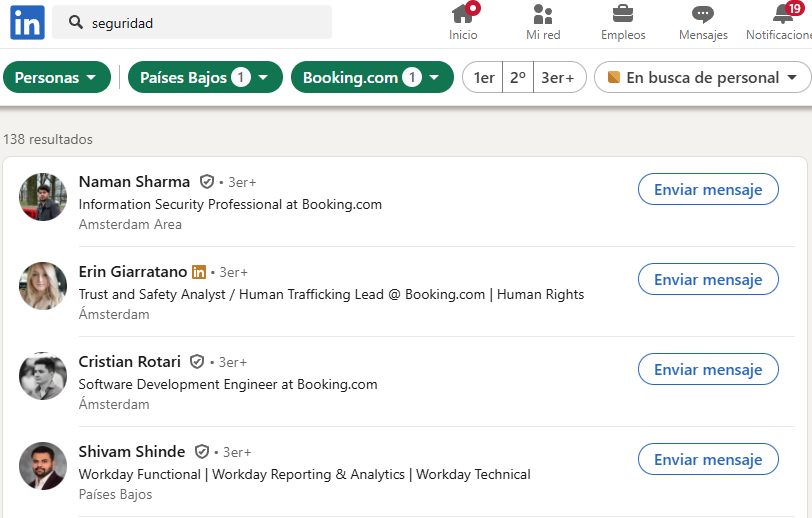
Los datos analizados en “Email Address” no muestran indicios de mail pertenecientes a roles importantes o puestos claves.

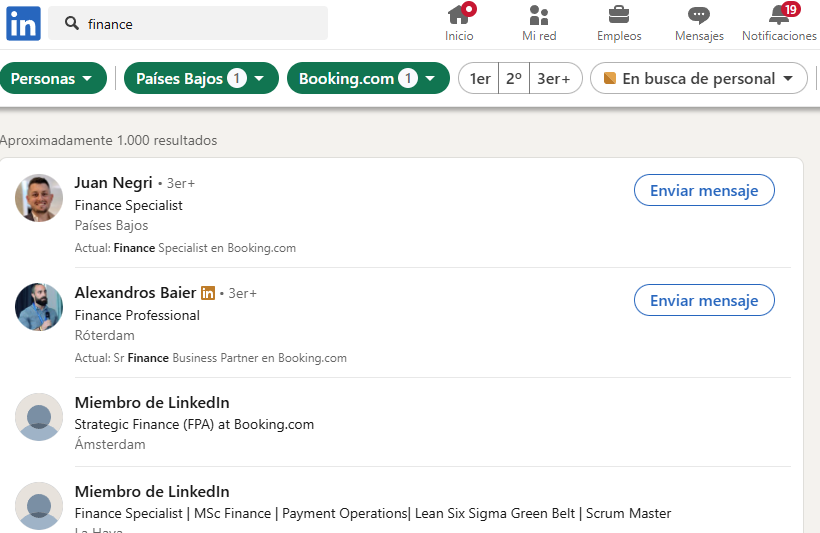
Haremos una búsqueda de posibles empleados en redes sociales, nos enfocaremos en la red **LinkedIn**. Utilizaremos los siguientes parámetros de búsqueda y exploraremos los resultados:



Conociendo el origen de la organización, Países Bajos, modificaremos los parámetros en busca de información:







# RESUMEN

### Objetivo

El informe pretende dejar en evidencia las herramientas y conocimientos adquiridos en el módulo, gestionando con diferentes técnicas de recopilación sobre un dominio definido.

En cada apartado se ha generado observaciones con una mirada crítica sobre posibles vulnerabilidades.

### Herramientas

Utilizamos las siguientes herramientas para explorar la información:

* Kali
* Shuffledns
* Analyticsrelationships
* Cero
* Katana
* CTFR
* Gau
* Alterx
* Dnsx
* Httpx
* Masscan
* Nmap
* Gowitness
* Wappalyzer
* Wafw00f
* Ffuf
* Greenbone
* Nuclei
* Wpscan
* Qualys -web-
* dmarcian.com -web-
* Subzy
* Maltego
* Spiderfoot
* Exiftool
* LinkedIn -web-

Se adjunta al informe el directorio “booking.com” y los respectivos ficheros de cada análisis.